Appl. No. 10/019,344 Amdt. dated Nov. 3, 2005 Reply to Office Action of August 18, 2005

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

10

11

12

Claims 1-14 (canceled)

- Claim 15 (new): A method for protecting a portable card, 1 provided with a cryptographic algorithm for enciphering data 2 and/or authenticating the card, against deriving a secret 3 key used in the card from statistical analysis of 4 information leaking away from the card to an outside world 5 in the event of cryptographic operations performed by the 6 card, the card being provided with at least a shift register 7 having linear and non-linear feedback functions for 8 implementing cryptographic algorithms, the method comprising 9 the steps of:
 - loading data to be processed and a secret key into the shift register of the card; and
- controlling the linear and non-linear feedback 13 functions in such a manner that collection of values of 14 recorded leak-information signals is resistant to deriving 15 the secret key through said statistical analysis of the 16 values. 17
- Claim 16 (new): The method recited in claim 15 wherein said 1
- manner comprises invoking the linear and non-linear feedback 2
- functions in a predefined sequence. 3

- Appl. No. 10/019,344 Amdt. dated Nov. 3, 2005 Reply to Office Action of August 18, 2005
- Claim 17 (new): The method recited in claim 15 wherein the
- 2 information leaking away to the outside world comprises
- either power-consumption data or electromagnetic radiation.
- Claim 18 (new): The method recited in claim 15 further
- 2 comprising the steps of:
- after the key has been loaded into the shift register,
- 4 clocking the shift register several times, during a specific
- 5 period, using at least the linear-feedback function;
- 6 then loading data into the shift register only using
- 7 the linear-feedback function; and
- subsequently clocking the shift register.
- Claim 19 (new): The method recited in claim 18 further
- comprising the step of:
- during a first instance of clocking the shift register,
- 4 clocking the shift register for a sufficiently long time
- such that the contents of all elements of the shift register
- 6 largely depend on bits of the key.
- Claim 20 (new): The method recited in claim 18 further
- comprising the steps of:
- after the key has been loaded into the shift register,
- disconnecting the data from an input to the shift register;
- 5 and
- after the specific period has occurred, reconnecting
- 7 the data to the input of the shift register so that the data
- 8 can then be loaded into the shift register.
- Claim 21 (new): The method recited in claim 15 further
- comprising the step of:

- Appl. No. 10/019,344 Amdt. dated Nov. 3, 2005 Reply to Office Action of August 18, 2005
- after the key has been loaded into the shift register,
- 4 clocking the shift register, during a specific period,
- several times, with the linear and non-linear feedback
- functions of the shift register being active but no data
- 7 being loaded into the shift register during or prior to the
- 8 clocking or prior to loading the key.
- Claim 22 (new): The method recited in claim 21 further
- comprising the steps of:
- after the key has been loaded into the shift register,
- disconnecting the data from an input to the shift register;
- 5 and
- 6 after the specific period has occurred, reconnecting
- the data to the input to the shift register so that the data
- 8 can then be loaded into the shift register.
- 1 Claim 23 (new): The method recited in claim 15 further
- comprising the step of:
- loading the key into the shift register with both the
- 4 linear and non-linear functions being active and only when
- 5 the contents of the shift register are fixed.
- Claim 24 (new): The method recited in claim 15 further
- comprising the steps of:
- if the key is not been loaded into the shift register
- 4 while the contents of the shift register are fixed, loading

Appl. No. 10/019,344 Amdt. dated Nov. 3, 2005 Reply to Office Action of August 18, 2005

- 5 the key into the shift register using only the linear
- 6 feedback function; and
- 7 then clocking the shift register.